A SESSION ON ARIZONA'S

ELECTRONIC NOTARY PUBLIC

HB 2242

2ND REGULAR SESSION, 44TH LEGISLATURE

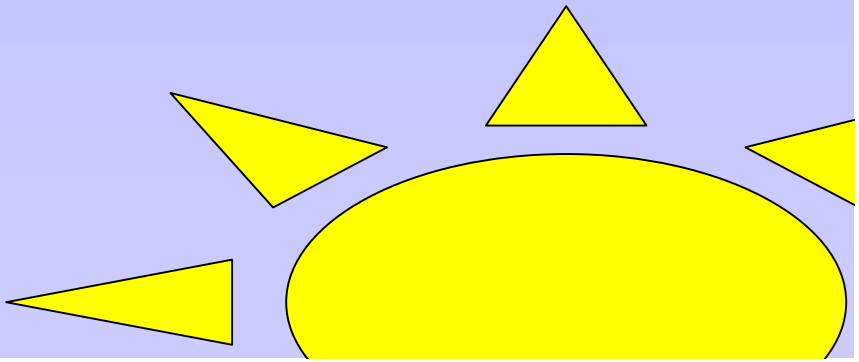
DAWN OF AN E-FUTURE . . .

Michael Totherow

Chief Information Officer

Office of the Secretary of State

mtotherow@sos.state.az.us



E-Signatures make E-Documents

Arizona Revised Statutes

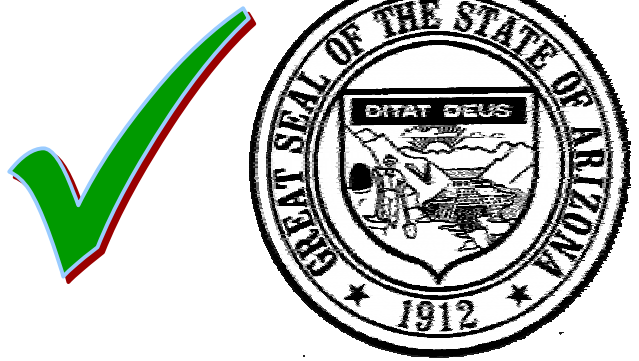
41-132. Electronic and digital signatures, exemptions, definitions

41-121. Duties (Secretary of State)

Paper Notary makes paper Document

Arizona Revised Statutes

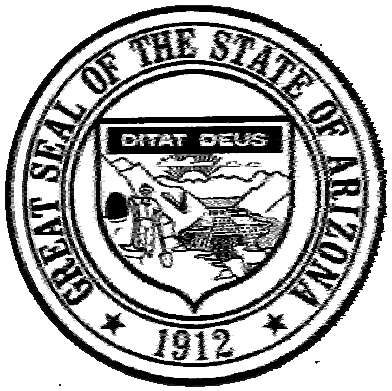
41-312. Appointment; term; oath and bond



E-Notary makes E-Document secure

Arizona Revised Statutes

41-132. Electronic and digital signatures, exemptions, definitions
41-121. Duties (Secretary of State)
41-312. Appointment; term; oath and bond



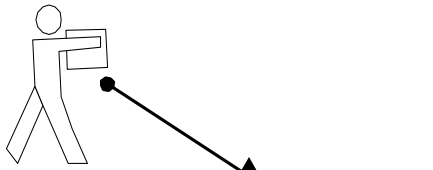
NOTARIAL ACTS

- **Acknowledgement** - a signer acknowledges before notary that they signed document
- **Oath or Affirmation** - person makes a vow in presence of notary under penalty of perjury
- **Copy certification** - notary makes a copy & certifies it as a copy of original
- **Jurat** - person attests to truthfulness of document signed before a notary

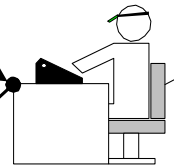
NOTARIAL CONCEPTS

- **Notarial Certificate** - part of or attachment to document for completion by notary (ie the signature and seal)
- **Identification** - identify individual through satisfactory evidence or personally known.
- **Notary Journal** - record of notarial acts completed by the notary
- **Neutrality** - notary is impartial witness to transaction.

TRADITIONAL NOTARY PROCESS

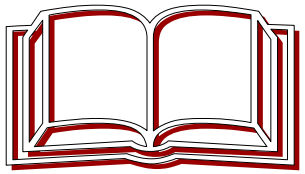


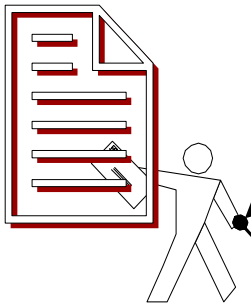
Person creates/has
document
needs notary



Notary

identify the person
perform notarial duty
notarial certificate
log in journal
collect fee





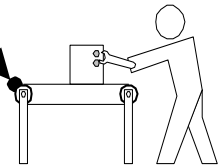
Person mails or
delivers
notarized document

Identify the person

perform notarial duty
take acknowledgment
administer oath or affirmation
perform jurat
perform copy certification

Notarial Certificate
affix seal and sign certificate,
on or attached to document

Log in Journal



Receipient receives the notarized
document

repeat as needed

ARIZONA

ELECTRONIC NOTARY PUBLIC

HB2242

TITLE: notary fees
(NOW: **electronic notarization act; fee**)

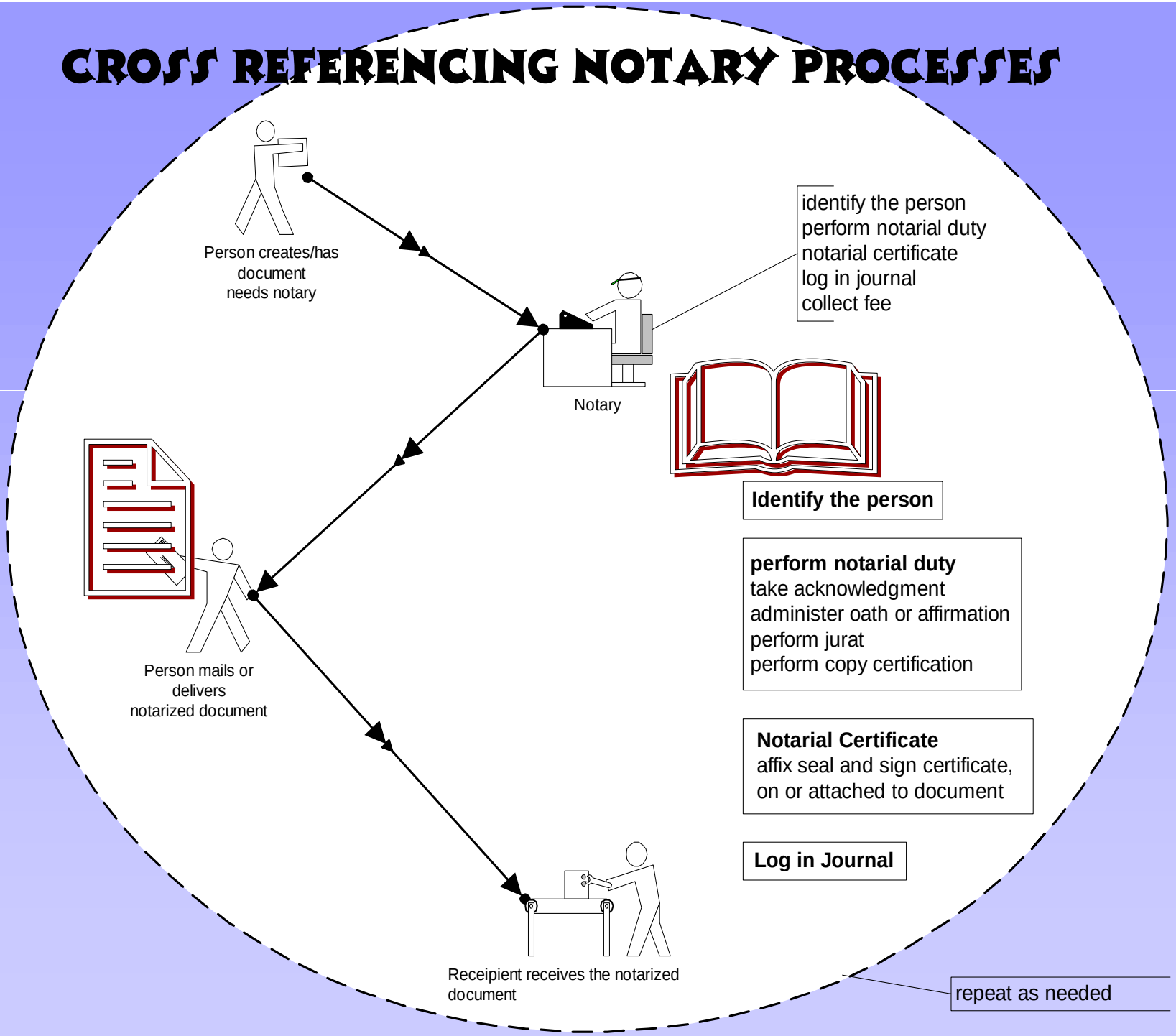
TRANSMITTED TO:	GOVERNOR	04/05/00
ACTION:	SIGNED	04/10/00

CHAPTER: 210
CHAPTERED VERSION: Senate Engrossed Version

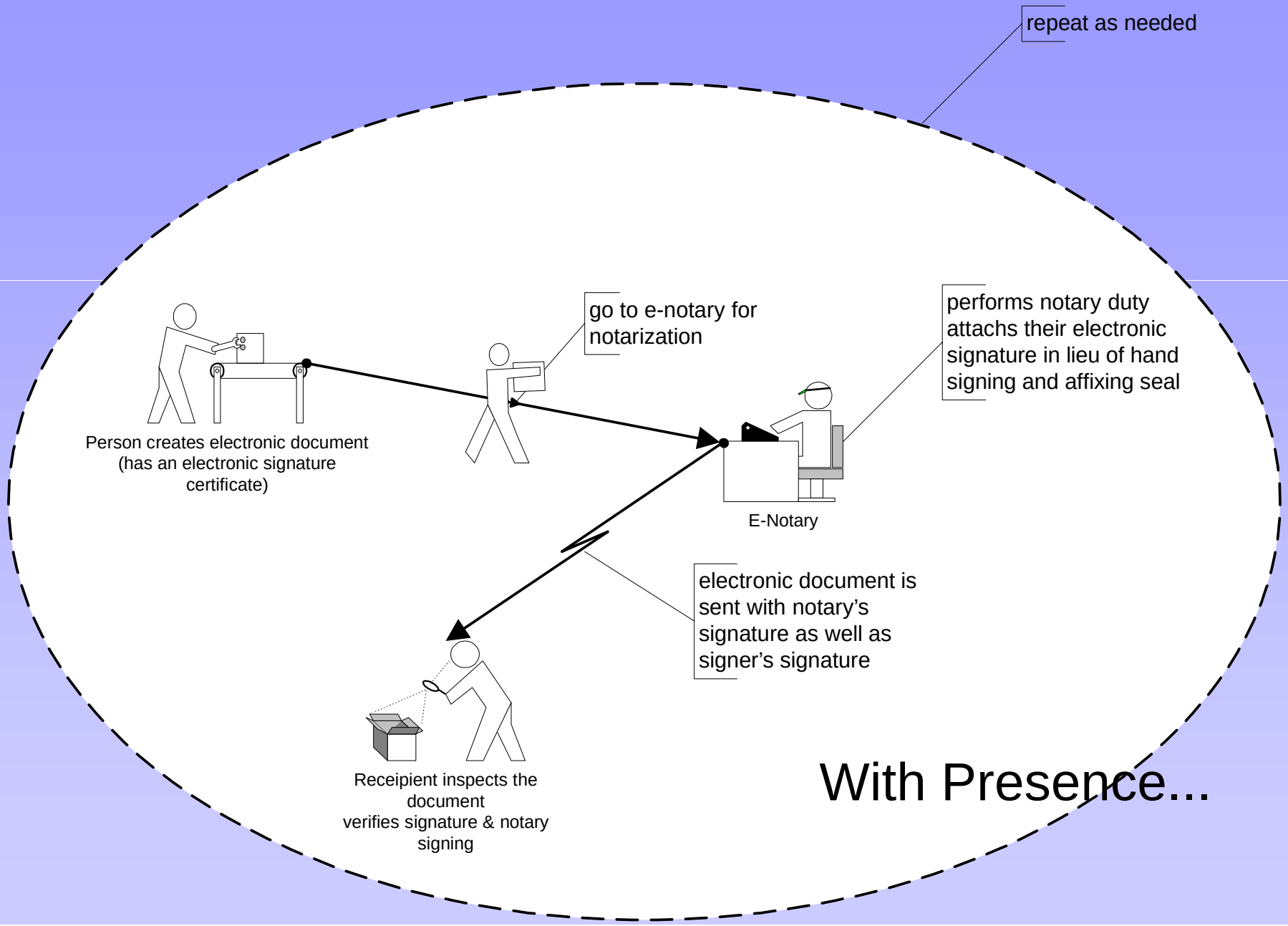
ELECTRONIC NOTARY LAW

- Same legal effect as paper notarial acts
- Same functions as paper notary
  - -Acknowledgement
  - -Copy certification
  - -Oath or affirmation
  - -Jurats
- Permits notarial acts either:
  - -with the presence of e-notary
  - -without the presence of an e-notary*
- Uses Electronic signature not rubber stamp

CROSS REFERENCING NOTARY PROCESSES



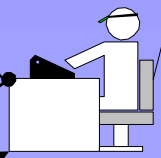
Notary Electronic Signature Process



Electronic Signature "Notary" Process

Person needs "notary" electronic signature certificate

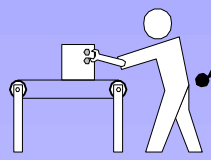
identify the person
perform Issuer duty
log in journal
collect fee



Certificate Issuer

repeat as needed

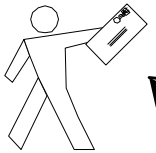
inband acknowledgment
verifies person has private key



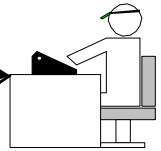
Person can create "notary" electronic signature certificate

signed electronic
document sent with
request for timestamp

performs timestamp duty
attachs timestamp token
log in journal



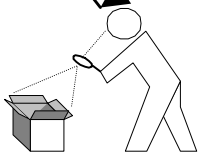
Person transmits or delivers electronic document



Trusted Third Party timestamps the document

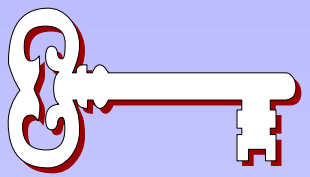
acknowledgement sent

timestamped document
sent to recepient



Receipient inspects the document
verifies signature & timestamp
sends acknowledgment of receipt

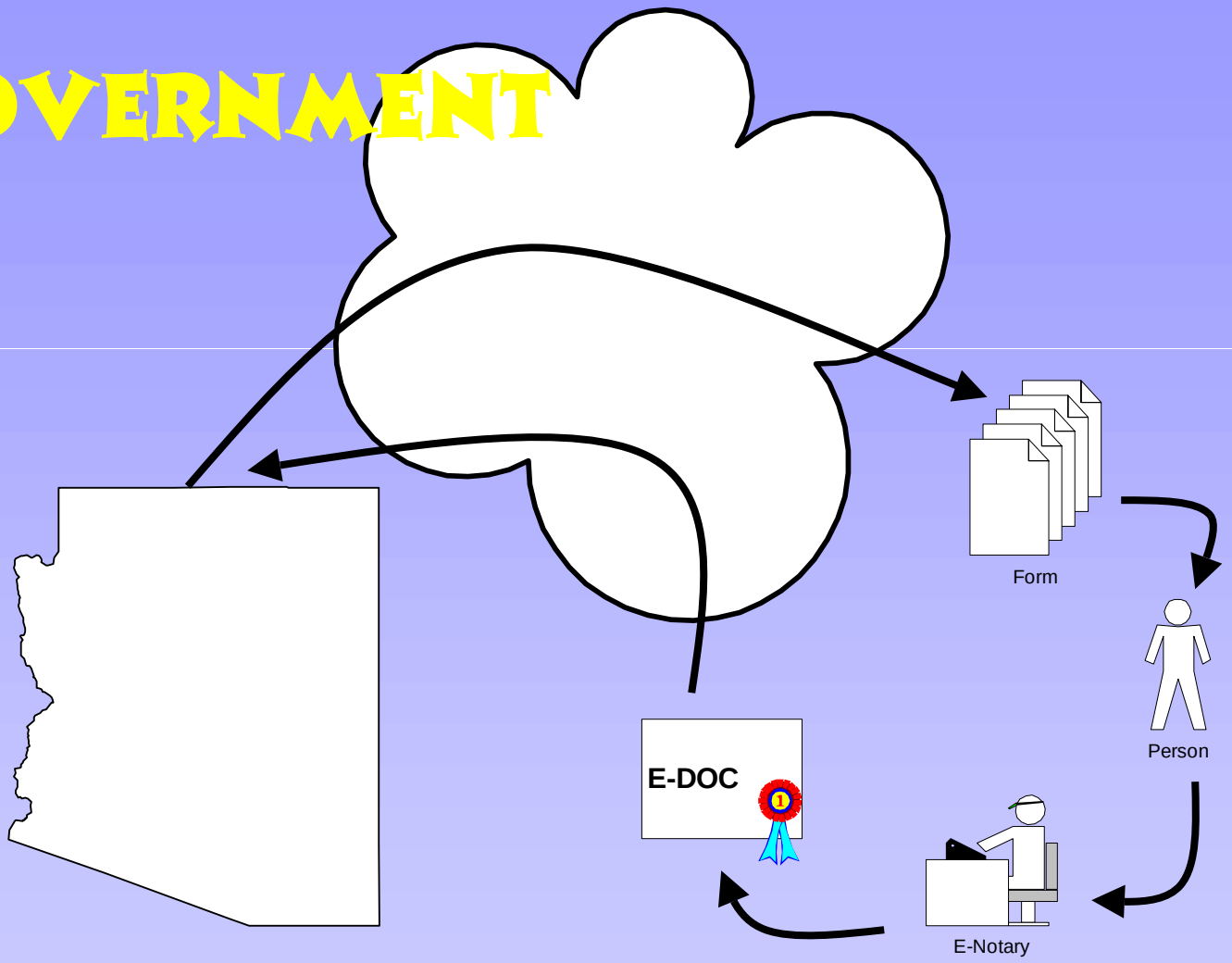
Without Presence...



NOTARIZED ELECTRONIC SIGNATURE TOOL

ARIZONA

E-GOVERNMENT



Electronic Document Equivalence of a Notary

The critical elements of notarizing a document are:

- affirming it is that person
- affirming they did sign & attest
- keep a record of the event

It can be argued that the use of a properly issued digital certificate will meet the first two elements. The third is met by having a "Trusted Third Party" time-stamp the document so that their signature and the time-date wrap the document such that it is readable but unalterable without destroying the trusted third party's signature.

The risk of repudiation is further reduced by having the receiving party send an acknowledgment to the signer. This will allow the signer to repudiate the signing at the time. If they do not, that is additional evidence of their intent to sign.

Arizona's Electronic Notary Act

Discussion of range of signatures allowed when e-notarize in the presence of an e-notary vs restricted signature forms allowed without the presence of an e-notary.

E-Sign and UETA are technology agnostic… so this process must account for multiple technologies.

ARIZONA'S ELECTRONIC NOTARY ACT

From a 11/28/00 press release:

Through a strategic alliance with Xco, the Yco Electronic Signature Service now includes a customized version of Xco's Assured Office. Yco's Electronic Signature Service now bundles an Yco Digital ID and its version of Assured Office, which allows users to electronically sign Microsoft(R) Word documents with embedded signatures. Signatures can also be attached to documents created in other applications, including HTML, PDF, JPEG, and more. Customers can purchase additional versions of Assured Office for signing Excel(R) and Adobe(R) documents. Digital IDs are required to make digital signature technology work.

...

Yco is a trusted third party that stands behind its customers in the same way that VISA(R) and other credit card companies stand behind merchants and consumers. By joining the Yco network, companies can avoid spending millions of dollars to build a similar in-house framework and dedicating the technical resources to manage it.

RECORDS MANAGEMENT GUIDANCE FOR IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES

- Electronic signature records need to be retained based on their operational needs and perceptions of risk.
- If an electronically signed record needs to be preserved, whether for a finite period of time or permanently, then its trustworthiness over time needs to be assured.
- Use of a records retention schedule needs to include
    - designating the disposition authority to dispose of records
    - the means to dispose of records at the end of the scheduled retention

TRUSTWORTHY RECORDS

Reliability - record content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.

Authenticity - a record proven to be what it purports to be and to have been created or sent by the person who purports to have created and sent it.

Usability - a record that can be located, retrieved, presented, and interpreted. In any subsequent retrieval and use, the record should be capable of being directly connected to the business activity or transaction which produced it. It should be possible to identify a record within the context of broader business activities and functions. The links between records which document a sequence of activities should be maintained. These contextual linkages of records should carry the information needed for an understanding of the transaction that created and used them.

TRUSTWORTHY RECORDS (cont)

Integrity - a record being complete and unaltered.

- protect record against alteration without appropriate permission.

- records management policies and procedures should specify
  - what, if any, additions or annotations may be made to a record after it is created,
  - under what circumstances additions or annotations may be authorized, and
  - who is authorized to make them.

- Any authorized annotation or addition to a record made after it is complete should be explicitly indicated as annotations or additions.

- structural integrity of a record - the structure of a record should remain physically or logically intact - its physical and logical format and the relationships between the data elements comprising the record. Failure to maintain the record's structural integrity may impair its reliability and authenticity.

PRESERVING TRUSTWORTHY RECORDS

For a record to remain reliable, authentic, with its integrity maintained, and useable over the record life cycle, it is necessary to preserve its content, context, and sometimes its structure.

A trustworthy record preserves the actual content of the record itself and information about the record that relates to the context in which it was created and used (e.g. formatting of presentation).

Specific contextual information will vary depending upon the business, legal, and regulatory requirements of the business.

It also may be necessary to preserve the structure or arrangement of its parts. Failure to preserve the structure of the record will impair its structural integrity. That may undermine the record's reliability and authenticity (e.g. Linking the parts of the record together - presentation organizational instructions such as what text with what graphic).

PRESERVING TRUSTWORTHY RECORDS

*Content**

- The electronic signature or signatures in a record are part of the content.
- They indicate who signed a record and whether that person approved the content of the record.
- Multiple signatures can indicate initial approval and subsequent concurrency.
- Signatures are often accompanied by dates and other identifiers such as organization or title.
- All of this is part of the content of the record and needs to be preserved.
- Lack of this information seriously affects a document's reliability and authenticity.

PRESERVING TRUSTWORTHY RECORDS

*Context**

- Some electronic signature technologies rely on individual identifiers that are not embedded in the content of the record, trust paths, and other means to create and verify the validity of an electronic signature. This information is outside of the *content* of the record, but is nevertheless important to the *context* of the record as it provides additional evidence to support the reliability and authenticity of the record.
- Lack of these contextual records seriously affects one's ability to verify the validity of the signed content.

PRESERVING TRUSTWORTHY RECORDS

*Structure**

- Preserving the structure of a record means its physical and logical format and the relationships between the data elements comprising the record remain physically and logically intact.
- It may be necessary to maintain the structure of the electronic signature. In that case it is necessary to retain the hardware and software that created the signature (e.g., chips or encryption algorithms) so that the complete record could be revalidated at a later time as needed.

* text largely from
"Records Management Guidance for Agencies Implementing Electronic Signature Technologies"
National Archives and Records Administration, Oct. 18, 2000

PRESERVING TRUSTWORTHY RECORDS

NON-REPUDIATION

Some form of technical non-repudiation services must be implemented to protect reliability, authenticity, integrity and usability.

Essential elements:

- Evidence of the origin of the message
- Evidence of sent
- Evidence of receipt
- Timestamp as needed of origin, sent, receipt
- Long-term storage of evidence
- Designated adjudicator of prospective disputes

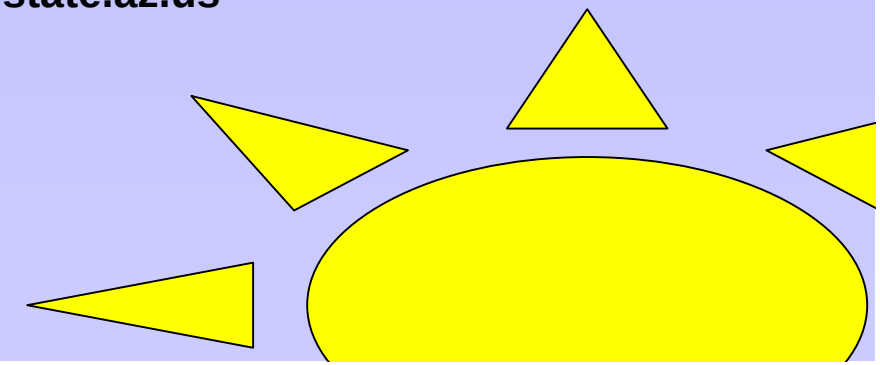
E-SIGN

UETA

E-NOTARY

A COMPLETE RECIPE FOR ELECTRONIC TRANSACTIONS

Russ Savage - Michael Totherow

rsavage@sos.state.az.us

mtotherow@sos.state.az.us